ON PRIMES IN ARITHMETIC PROGRESSIONS

ZHI-WEI SUN

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
`http://math.nju.edu.cn/~zwsun`

ABSTRACT. Let $d \geqslant 4$ and $c \in (-d, d)$ be relatively prime integers, and let $r(d)$ be the radical of d. We show that for any sufficiently large integer n (in particular $n > 24310$ suffices for $4 \leqslant d \leqslant 36$), the least positive integer m with $2r(d)k(dk - c)$ $(k = 1, \dots, n)$ pairwise distinct modulo m is just the first prime $p \equiv c \pmod{d}$ with $p \geqslant (2dn - c)/(d - 1)$. We also conjecture that for any integer $n > 4$ the least positive integer m such that $|\{k(k-1)/2 \bmod m : k = 1, \dots, n\}| = |\{k(k-1)/2 \bmod m + 2 : k = 1, \dots, n\}| = n$ is just the least prime $p \geqslant 2n - 1$ with $p + 2$ also prime.

1. INTRODUCTION

To find nontrivial arithmetical functions taking only prime values is a fascinating topic in number theory. In 1947 W. H. Mills [M] showed that there exists a real number A such that $\lfloor A^{3^n} \rfloor$ is prime for every $n \in \mathbb{Z}^+ = \{1, 2, 3, \dots\}$; unfortunately such a constant A cannot be effectively found.

For each integer $h > 1$ and sufficiently large integer n, it was determined in [BSW] the least positive integer m with $1^h, 2^h, \dots, n^h$ pairwise distinct modulo m, but such integers m are composite infinitely often. In a recent paper [S] the author proved that the smallest integer $m > 1$ such that those $2k(k - 1) \bmod m$ for $k = 1, \dots, n$ are pairwise distinct, is just the least prime greater than $2n - 2$, and that for $n \in \{4, 5, \dots\}$ the least positive integer m such that $18k(3k - 1)$ $(k = 1, \dots, n)$ are pairwise distinct modulo m. is just the least prime $p > 3n$ with $p \equiv 1 \pmod 3$. When $d \in \{4, 5, 6, \dots\}$ and $c \in (-d, d)$ are relatively prime, it is natural to ask whether there is a similar result for primes in the arithmetic progression $\{c, c+d, c+2d, \dots\}$ since there are infinitely many such primes by Dirichlet's theorem.

In this paper we establish the following general theorem.

1

Theorem 1.1. *Let $d \geqslant 4$ and $c \in (-d, d)$ be relatively prime integers, and let $r(d)$ be the radical of d (i.e., the product of all the distinct prime divisors of d).*

(i) *For any sufficiently large integer n, the least positive integer m with $2r(d)k(dk - c)$ $(k = 1, \ldots, n)$ pairwise distinct modulo m is just the first prime $p \equiv c \pmod{d}$ with $p \geqslant (2dn - c)/(d - 1)$.*

(ii) *When $4 \leqslant d \leqslant 36$ and $n > M_d$, the required result in the first part holds, where*

$$M_4 = 8, \ M_5 = 14, \ M_6 = 10, \ M_7 = 100, \ M_8 = 21, \ M_9 = 315, \ M_{10} = 53,$$
$$M_{11} = 1067, \ M_{12} = 27, \ M_{13} = 1074, \ M_{14} = 122, \ M_{15} = 809, \ M_{16} = 329,$$
$$M_{17} = 5115, \ M_{18} = 95, \ M_{19} = 5390, \ M_{20} = 755, \ M_{21} = 3672, \ M_{22} = 640,$$
$$M_{23} = 11193, \ M_{24} = 220, \ M_{25} = 12810, \ M_{26} = 1207, \ M_{27} = 7087,$$
$$M_{28} = 2036, \ M_{29} = 13250, \ M_{30} = 177, \ M_{31} = 24310, \ M_{32} = 3678,$$
$$M_{33} = 12794, \ M_{34} = 5303, \ M_{35} = 15628, \ M_{36} = 551.$$

Remark 1.1. To obtain the effective lower bounds M_d $(4 \leqslant d \leqslant 36)$ in part (ii) of Theorem 1.1, we actually employ some computational results of O. Ramaré and R. Rumely [RR] on primes in arithmetic progressions. Define

$$c_4 = -3, \ c_5 = -1, \ c_6 = 1, \ c_7 = -5, \ c_8 = 1, \ c_9 = 2, \ c_{10} = 3,$$
$$c_{11} = -7, \ c_{12} = 5, \ c_{13} = -5, \ c_{14} = -5, \ c_{15} = -1, \ c_{16} = 11,$$
$$c_{17} = 15, \ c_{18} = 1, \ c_{19} = 6, \ c_{20} = -9, \ c_{21} = 1, \ c_{22} = 5,$$
$$c_{23} = 21, \ c_{24} = 1, \ c_{25} = 19, \ c_{26} = -3, \ c_{27} = 23,$$
$$c_{28} = -9, \ c_{29} = -1, \ c_{30} = 17, \ c_{31} = 3, \ c_{32} = -1,$$
$$c_{33} = -5, \ c_{34} = 15, \ c_{35} = 12, \ c_{36} = 23.$$

Then, for every $d = 4, \ldots, 36$ the smallest positive integer m such that $2r(d)k(dk - c_d)$ $(k = 1, \ldots, M_d)$ are pairwise incongruent modulo m is *not* the least prime $p \equiv c_d \pmod{d}$ with $p \geqslant (2dn - c_d)/(d - 1)$.

Here we give a simple consequence of Theorem 1.1.

Corollary 1.1. (i) *For each integer $n \geqslant 6$, the least positive integer m such that $4k(4k - 1)$ (or $4k(4k + 1)$) for $k = 1, \ldots, n$ are pairwise distinct modulo m, is just the least prime $p \equiv 1 \pmod{4}$ with $p \geqslant (8n - 1)/3$ (resp., $p \equiv -1 \pmod{4}$ with $p \geqslant (8n + 1)/3$).*

(ii) *Let $C_1 = 8$, $C_2 = 10$, $C_3 = 15$ and $C_{-2} = 5$. For any $r \in \{\pm 1, \pm 2\}$ and integer $n \geqslant C_r$, the least positive integer m such that $10k(5k - r)$ for $k = 1, \ldots, n$ are pairwise distinct modulo m, is just the least prime $p \equiv r \pmod{5}$ with $p \geqslant (10n - r)/4$.*

As a supplement to Theorem 1.1, we are able to prove the following result for the cases $d = 2, 3$.

Theorem 1.2. (i) *For any integer $n \geqslant 5$, the smallest positive integer m such that those $4k(2k-1)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is the least prime or power of 2 not smaller than $4n-1$. Also, for any integer $n \geqslant 7$, the smallest positive integer m such that those $4k(2k+1)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is the least prime or power of 2 not smaller than $4n$.*

(ii) *For any integer $n \geqslant 4$, the smallest positive integer m such that those $6k(3k-1)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is the least prime $p \equiv 1 \pmod 3$ or power of 3 not smaller than $3n$; for any integer $n \geqslant 5$, the smallest positive integer m such that those $6k(3k+1)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is the least prime $p \equiv 2 \pmod 3$ or power of 3 not smaller than $3n$. Also, for any integer $n \geqslant 3$, the smallest positive integer m such that those $6k(3k-2)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is the least prime $p \equiv 2 \pmod 3$ or power of 3 not smaller than $3n-1$, and for any integer $n \geqslant 8$, the smallest positive integer m such that those $6k(3k+2)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is the least prime $p \equiv 1 \pmod 3$ or power of 3 not smaller than $3n$.*

Remark 1.2. As Theorem 1.2 can be proved by the method in [S], and it is less important than Theorem 1.1, in this paper we omit its proof. We are also able to show that for any integer $n \geqslant 3$ the smallest positive integer m such that $8k(2k-1)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is just the least prime $p \geqslant 4n-1$, and that for any integer $n \geqslant 9$ the smallest positive integer m such that $8k(2k+1)$ $(k=1,\ldots,n)$ are pairwise distinct modulo m is just the least prime $p \geqslant 4n+1$.

To conclude this section we pose some new conjectures.

Conjecture 1.1. *For any $d \in \mathbb{Z}^+$ there is a positive integer n_d such that for any integer $n \geqslant n_d$ the least positive integer m satisfying*

$$\left| \left\{ \binom{k}{2} \bmod m : \ k=1,\ldots,n \right\} \right| = \left| \left\{ \binom{k}{2} \bmod m+2d : \ k=1,\ldots,n \right\} \right| = n$$

is just the first prime $p \geqslant 2n-1$ with $p+2d$ also prime. Moreover, we may take

$$n_1 = 5, \ n_2 = n_3 = 6, \ n_4 = 10, \ n_5 = 9,$$
$$n_6 = 8, \ n_7 = 9, \ n_8 = 18, \ n_9 = 11, \ n_{10} = 9.$$

Remark 1.3. A well known conjecture of de Polignac [P] asserts that for any positive integer d there are infinitely many prime pairs $\{p,q\}$ with $p-q=2d$.

Conjecture 1.2. *Let n be any positive integer and take the least positive integer m such that*

$$\left|\left\{\binom{k}{2} \bmod m: \ k=1,\ldots,n\right\}\right| = \left|\left\{\binom{k}{2} \bmod m+1: \ k=1,\ldots,n\right\}\right| = n.$$

Then, each of m and $m+1$ is either a power of two (including $2^0 = 1$) or a prime times a power of two.

Conjecture 1.3. *Let n be any positive integer. Then the least positive integer m of the form $x^2 + x + 1$ (or $4x^2 + 1$) such that those $\binom{k}{2}$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, is just the the first prime $p \geqslant 2n - 1$ of the form $x^2 + x + 1$ (or $4x^2 + 1$)*

Remark 1.4. The conjecture that there are infinitely many primes of the form $x^2 + x + 1$ (or $4x^2 + 1$) is still open. We may also replace $\binom{k}{2}$ in Conjecture 1.3 by k^2.

Conjecture 1.4. *For any integer $n > 2$, the smallest positive integer m such that those $6p_k(p_k - 1)$ $(k = 1, \ldots, n)$ are pairwise incongruent modulo m is just the first prime $p \geqslant p_n$ dividing none of those $p_i + p_j - 1$ $(1 \leqslant i < j \leqslant n)$, where p_k denotes the k-th prime.*

Remark 1.5. For any prime $p \geqslant p_n$ dividing none of those $p_i + p_j - 1$ $(1 \leqslant i < j \leqslant n)$, clearly $p_j(p_j - 1) - p_i(p_i - 1) = (p_j - p_i)(p_i + p_j - 1) \not\equiv 0 \pmod{p}$ for all $1 \leqslant i < j \leqslant n$.

We also have some other conjectures similar to Conjectures 1.1–1.4.

In the next section we provide some lemmas. Section 3 is devoted to our proof of Theorem 1.1.

2. Some lemmas

Lemma 2.1. *Let c and $d > 0$ be relatively prime integers. For any $\varepsilon > 0$, if $n \in \mathbb{Z}^+$ is large enough, then there is a prime $p \equiv c \pmod{d}$ with*

$$\frac{d(2n - 1) - c}{d - 1} < p \leqslant \frac{d((2 + \varepsilon)n - 1) - c}{d - 1}.$$

Proof. By the Prime Number Theorem for arithmetic progressions (cf. (1.5) of [CP, p. 13] or Theorem 4.4.4 of [J, p. 175]),

$$\pi(x; c, d) := |\{p \leqslant x: \ p \text{ is a prime with } p \equiv c \pmod{d}\}| \sim \frac{x}{\varphi(d) \log x}$$

as $x \to +\infty$, where φ is Euler's totient function. Note that

$$\lim_{n \to +\infty} \frac{d((2 + \varepsilon)n - 1) - c}{d - 1} \Big/ \frac{d(2n - 1) - c}{d - 1} = \frac{2 + \varepsilon}{2}$$

and

$$\log \frac{d((2+\varepsilon)n-1)-c}{d-1} \sim \log n \sim \log \frac{d(2n-1)-c}{d-1}.$$

Thus

$$\lim_{n \to +\infty} \pi\left(\frac{d((2+\varepsilon)n-1)-c}{d-1}; c, d\right) \Big/ \pi\left(\frac{d(2n-1)-c}{d-1}; c, d\right) = 1 + \frac{\varepsilon}{2} > 1.$$

It follows that

$$\pi\left(\frac{d((2+\varepsilon)n-1)-c}{d-1}; c, d\right) > \pi\left(\frac{d(2n-1)-c}{d-1}; c, d\right)$$

for all sufficiently large $n \in \mathbb{Z}^+$. This ends the proof. $\square$

Lemma 2.2. *Let $d > 2$ and $c \in (-d, d)$ be relatively prime integers. Suppose that p is a prime not exceeding $(d((2+\varepsilon)n-1)-c)/(d-1)$ where $n \geqslant 3d$ and $0 < \varepsilon \leqslant 2/(d-2)$. Then those $2r(d)k(dk-c)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo p if and only if $p \equiv c \pmod d$ and $p > (d(2n-1)-c)/(d-1)$.*

Proof. If $p \mid 2d$, then $p \mid 2r(d)$ and hence all those $2r(d)k(dk-c)$ $(k = 1, \ldots, n)$ cannot be pairwise distinct modulo p. Note that $(d(2n-1)-c)/(d-1) \geqslant (3d-c)/(d-1) \geqslant 2d/(d-1) > 2$. If $p \mid d$ then $p \not\equiv c \pmod d$.

Now assume that $p \nmid 2d$, $p \not\equiv c \pmod d$ or $p \leqslant (d(2n-1)-c)/(d-1)$. Then $jp \equiv -c \pmod d$ for some $1 \leqslant j \leqslant d-1$. Write $jp + c = dq$ with $q \in \mathbb{Z}$. If $p \not\equiv c \pmod d$, then $j \leqslant d-2$ and hence

$$q \leqslant \frac{c}{d} + \frac{d-2}{d}p \leqslant \frac{c}{d} + \frac{d-2}{d} \cdot \frac{d((2+\varepsilon)n-1)-c}{d-1}$$
$$\leqslant \frac{c-d(d-2)}{d(d-1)} + \frac{d-2}{d-1}\left(2 + \frac{2}{d-2}\right)n < 2n.$$

If $p \equiv c \pmod d$ and $p \leqslant (d(2n-1)-c)/(d-1)$, then $j = d-1$ and $q \leqslant 2n-1$. If $q > 2$, then $0 < k := \lfloor (q-1)/2 \rfloor < l := \lfloor (q+2)/2 \rfloor \leqslant n$ and

$$d(k+l) - c = dq - c = jp \equiv 0 \pmod p$$

and hence

$$2r(d)l(dl-c) - 2r(d)k(dk-c) = 2r(d)(l-k)(d(k+l)-c) \equiv 0 \pmod p.$$

If $q \leqslant 2$, then $p \leqslant jp = dq - c \leqslant 2d - c < 3d \leqslant n$ and

$$2r(d)(p+1)(d(p+1)-c) - 2r(d)1(d \cdot 1 - c) = 2r(d)p(d(p+2)-c) \equiv 0 \pmod p.$$

Below we suppose that $p \nmid 2d$, $p \equiv c \pmod d$ and $p > (d(2n-1)-c)/(d-1)$. Then $(d-1)p + c = dq$ for some $q \geqslant 2n$. For any $1 \leqslant k < l \leqslant n$, we have

$$0 < l - k < n \leqslant \frac{dq}{2d} = \frac{(d-1)p+c}{2d} < \frac{p+1}{2} \leqslant p,$$

also $d(k+l) - c \leqslant d(2n-1) - c < (d-1)p$ and hence $d(k+l) \not\equiv c \pmod p$ since $jp \equiv jc \not\equiv -c \pmod d$ for all $j = 1, \ldots, d-2$. So, all those $2r(d)k(dk-c)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo p.

The proof of Lemma 2.2 is now complete.

Lemma 2.3. *Let $d > 2$ and $c \in (-d, d)$ be relatively prime integers, and let $n \geqslant 6d$ be an integer. Suppose that $m \in [n, (d((2 + \varepsilon)n - 1) - c)/(d - 1)]$ is a power of two or twice an odd prime, where $0 < \varepsilon \leqslant 2/3$. Then, there are $1 \leqslant k < l \leqslant n$ such that $2r(d)k(dk - c) \equiv 2r(d)l(dl - c) \pmod{m}$.*

Proof. Note that $m \geqslant n \geqslant 6d > 4$ and

$$\frac{m}{4} \leqslant \frac{d((2 + \varepsilon)n - 1) - c}{4(d - 1)} < \frac{d(2 + \varepsilon)}{4(d - 1)}n \leqslant \frac{d(2 + 2/3)}{4(d - 1)}n = \frac{8dn}{8d + 4(d - 3)} \leqslant n.$$

If d is even and m is a power of two, then for $k = 1$ and $l = m/4 + 1 \leqslant n$ we have

$$2r(d)l(dl - c) - 2r(d)k(dk - c) = 2r(d)(l - k)(d(l + k) - c) \equiv 0 \pmod{m}.$$

If $m = 2p$ with p an odd prime dividing d, then $m \mid 2r(d)$ and hence the desired result holds trivially.

In the remaining case, d and $m/2$ are relatively prime. Thus $jd \equiv c \pmod{m/2}$ for some $j = 1, \ldots, m/2$. If $j \leqslant 2$, then

$$\frac{m}{2} \leqslant jd - c \leqslant 2d - c < 3d \leqslant \frac{n}{2}$$

which contradicts $m \geqslant n$. So $3 \leqslant j \leqslant m/2$ and hence

$$0 < k := \left\lfloor \frac{j - 1}{2} \right\rfloor < l := \left\lfloor \frac{j + 2}{2} \right\rfloor \leqslant \frac{m}{4} + 1 < n + 1.$$

Note that $d(k + l) - c = jd - c \equiv 0 \pmod{m/2}$ and hence

$$2r(d)l(dl - c) - 2r(d)k(dk - c) = 2r(d)(l - k)(d(k + l) - c) \equiv 0 \pmod{m}.$$

This concludes the proof. $\square$

3. Proof of Theorem 1.1

Proof of Theorem 1.1. Let $\varepsilon = 2/(\max\{11, d\} - 2)$. By Lemma 2.1, there is an integer $N \geqslant \max\{6d, 243\}$ such that for any $n \geqslant N$ there is at least a prime $p \equiv c \pmod{d}$ with

$$\frac{d(2n - 1) - c}{d - 1} < p \leqslant \frac{d((2 + \varepsilon)n - 1) - c}{d - 1}. \tag{3.1}$$

When $p \equiv c \pmod{d}$, clearly $(d-1)p > d(2n-1)-c$ if and only if $(d-1)p \geqslant 2dn$.

(i) Fix an integer $n \geqslant N$ and take the least $m \in \mathbb{Z}^+$ such that those $2r(d)k(dk - c)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m. Clearly $m \geqslant n$.

By Lemma 2.2, $m \leqslant m'$ where m' denotes the first prime $p \equiv c \pmod{d}$ satisfying (3.1).

Assume that $m \neq m'$. We want to deduce a contradiction. Clearly m is not a prime by Lemma 2.2. Note that $\varepsilon \leqslant 2/9$. In view of Lemma 2.3, m is neither a power of two nor twice an odd prime. So we have $m = pq$ for some odd prime p and integer $q > 2$. Observe that

$$\frac{m}{3} \leqslant \frac{d((2+\varepsilon)n - 1) - c}{3(d-1)} < \frac{d(2+2/9)}{3(d-1)}n = \frac{20d}{27(d-1)}n \leqslant \frac{80}{81}n$$

and hence

$$\frac{m}{3} + 3 < \frac{80}{81}n + \frac{n}{81} = n. \tag{3.2}$$

If $p \mid d$, then for $k := 1$ and $l := q + 1 = m/p + 1 < m/3 + 3 < n$, we have $pq \mid r(d)(l-k)$ and hence

$$r(d)l(dl - c) - r(d)k(dk - c) = r(d)(l-k)(d(l+k) - c) \equiv 0 \pmod{m}.$$

Now suppose that $p \nmid d$. Then $2dk \equiv c - dq \pmod{p}$ for some $1 \leqslant k \leqslant p$, and $l := k + q \leqslant p + q = m/q + m/p$. Note that

$$(l-k)(d(l+k) - c) = q(d(2k+q) - c) \equiv 0 \pmod{pq}$$

and hence $2r(d)l(dl - c) \equiv 2r(d)k(dk - c) \pmod{m}$. If $\min\{p, q\} \leqslant 4$, then

$$l \leqslant p + q = \frac{m}{\min\{p,q\}} + \min\{p,q\} \leqslant \frac{m}{3} + 4 < n + 1$$

by (3.2). If $\min\{p, q\} \geqslant 5$, then

$$l \leqslant p + q = \frac{m}{q} + \frac{m}{p} \leqslant \max\left\{\frac{1}{6} + \frac{1}{7}, \frac{1}{5} + \frac{1}{8}\right\}m < \frac{m}{3} < n$$

since $pq = m \geqslant n \geqslant 243 \geqslant 40$. So we get a contradiction as desired.

(ii) Now assume that $4 \leqslant d \leqslant 36$ and $n > M_d$. By Table 1 of [RR, p. 419], we have

$$(1 - \varepsilon_d)\frac{x}{\varphi(d)} \leqslant \theta(x; c, d) \leqslant (1 + \varepsilon_d)\frac{x}{\varphi(d)}$$

for all $x \geqslant 10^{10}$, where φ denotes Euler's totient function, $\theta(x; c, d) := \sum_{p \leqslant x} \log p$ with p prime, and

$$\varepsilon_4 = 0.002238, \ \varepsilon_5 = 0.002785, \ \varepsilon_6 = 0.002238, \ \varepsilon_7 = 0.003248, \ \varepsilon_8 = 0.002811,$$
$$\varepsilon_9 = 0.003228, \ \varepsilon_{10} = 0.002785, \ \varepsilon_{11} = 0.004125, \ \varepsilon_{12} = 0.002781, \ \varepsilon_{13} = 0.004560,$$
$$\varepsilon_{14} = 0.003248, \ \varepsilon_{15} = 0.008634, \ \varepsilon_{16} = 0.008994, \ \varepsilon_{17} = 0.010746, \ \varepsilon_{18} = 0.003228,$$
$$\varepsilon_{19} = 0.011892, \ \varepsilon_{20} = 0.008501, \ \varepsilon_{21} = 0.009708, \ \varepsilon_{22} = 0.004125, \ \varepsilon_{23} = 0.012682,$$
$$\varepsilon_{24} = 0.008173, \ \varepsilon_{25} = 0.012214, \ \varepsilon_{26} = 0.004560, \ \varepsilon_{27} = 0.011579, \ \varepsilon_{28} = 0.009908,$$
$$\varepsilon_{29} = 0.014102, \ \varepsilon_{30} = 0.008634, \ \varepsilon_{31} = 0.014535, \ \varepsilon_{32} = 0.011103, \ \varepsilon_{33} = 0.011685,$$
$$\varepsilon_{34} = 0.010746, \ \varepsilon_{35} = 0.012809, \ \varepsilon_{36} = 0.009544.$$

Recall that $\varepsilon = 2/(\max\{11, d\} - 2)$. If $n \geqslant 10^{10}/2$, then we can easily verify that

$$\frac{\varepsilon}{2} - \frac{1}{n} \geqslant \frac{\varepsilon}{2} - \frac{2}{10^{10}} > \frac{2\varepsilon_d}{1 - \varepsilon_d} = \frac{1 + \varepsilon_d}{1 - \varepsilon_d} - 1,$$

thus

$$\frac{\theta(((2 + \varepsilon)n - 2)d/(d - 1); c, d)}{\theta(2nd/(d - 1); c, d)}$$

$$\geqslant \frac{(1 - \varepsilon_d)((2 + \varepsilon)n - 2)d/(d - 1)}{(1 + \varepsilon_d)2nd/(d - 1)} = \frac{1 - \varepsilon_d}{1 + \varepsilon_d}\left(1 + \frac{\varepsilon}{2} - \frac{1}{n}\right) > 1$$

and hence there is a prime $p \equiv c \pmod{d}$ with

$$\frac{d(2n - 1) - c}{d - 1} < \frac{2dn}{d - 1} < p \leqslant \frac{((2 + \varepsilon)n - 2)d}{d - 1} < \frac{d((2 + \varepsilon)n - 1) - c}{d - 1}.$$

Let N_d be the least positive integer such that for any $n = N_d, \ldots, 10^{10}/2$ and any $a \in \mathbb{Z}$ relatively prime to d, the interval $(2dn/(d-1), ((2+\varepsilon)n-2)d/(d-1))$ contains a prime congruent to a modulo d. Via a computer we find that

$$N_4 = 79, \ N_5 = 206, \ N_6 = 103, \ N_7 = 333, \ N_8 = 301, \ N_9 = 356, N_{10} = 232,$$
$$N_{11} = 1079, \ N_{12} = 346, \ N_{13} = 1166, \ N_{14} = 806, \ N_{15} = 1310, \ N_{16} = 2183,$$
$$N_{17} = 5153, \ N_{18} = 1135, \ N_{19} = 5402, \ N_{20} = 2388, \ N_{21} = 4059, \ N_{22} = 2934,$$
$$N_{23} = 11246, \ N_{24} = 2480, \ N_{25} = 13144, \ N_{26} = 4775, \ N_{27} = 11646,$$
$$N_{28} = 5314, \ N_{29} = 13478, \ N_{30} = 5215, \ N_{31} = 24334, \ N_{32} = 8964,$$
$$N_{33} = 15044, \ N_{34} = 14748, \ N_{35} = 16896, \ N_{36} = 9847.$$

For $n \geqslant N = \max\{N_d, 243\}$, we may apply part (i) to get the desired result. If $M_d < n \leqslant \max\{N_d, 243\}$, then we can easily verify the desired result via a computer.

In view of the above, we have completed the proof of Theorem 1.1. $\square$

References

[BSW] P. S. Bremser, P. D. Schumer and L. C. Washington, *A note on the incongruence of consecutive integers to a fixed power*, J. Number Theory **35** (1990), 105–108.

[CP] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, 2nd Edition, Springer, New York, 2005.

[J] G.J.O. Jameson, *The Prime Number Theorem*, Cambridge Univ. Press, Cambridge, 2003.

[M] W. H. Mills, *A prime-representing function*, Bull. Amer. Math. Soc. **53** (1947), 604.

[P] A. de Polignac, *Six propositions arithmologiques déduites de crible d'Ératosthene*, Nouv. Ann. Math. **8** (1849), 423–429.

[RR] O. Ramaré and R. Rumely, *Primes in arithmetic progressions*, Math. Comp. **65** (1996), 397–425.

[S] Z.-W. Sun, *On functions taking only prime values*, J. Number Theory **133** (2013), 2794–2812.